Jurnal Teknovasi
Volume 08, Nomor 01, 2021, 65 – 69
ISSN: 2540-8389

PENGAMANAN PESAN MENGGUNAKAN ALGORITMA DATA ENCRYPTION STANDARD (DES)

Fahmi Ruziq
Prodi Informatika
Universitas Battuta, Jl. Gajah Mada No. 15 M, Medan
E-mail: fahmiruziq89@gmail.com

ABSTRACT

Cryptography is an encryption technique, where the data to be encrypted will be encrypted using a key to become data that is difficult to read by other parties who do not have a decryption key. The DES algorithm is a symmetric block cipher cryptographic algorithm that uses a block size of 64 bits and a key size of 56 bits. In this study the DES algorithm will be used to encrypt messages. The result of this research is that the length of the file characters is directly proportional to the encryption and decryption process.

Keywords : *Cryptography, Data Encryption Standard (DES)*

PENDAHULUAN

Komunikasi merupakan salah satu dari sekian banyak sifat dasar manusia yang menjadi sarana saling pengertian antara satu dengan yang lain. Seiring dengan perkembangan zaman, cara komunikasi manusia terus berkembang. Pertukaran pesan antar orang dapat dilakukan dengan berbagai cara seperti bertukar pesan dalam bentuk teks baik berupa dokumen, gambar, portable document file (PDF), ataupun dalam bentuk lainnya. Keamanan pesan dan informasi sangat penting dalam berkomunikasi. Banyak kejahatan dunia maya mencari celah keamanan untuk memasuki dan memanipulasi pesan. Keamanan dan kerahasiaan pesan adalah prioritas. Dalam menjamin keamanan dan kerahasiaan pesan, diperlukan suatu teknik penyandian pesan atau informasi yang disebut kriptografi. Kriptografi merupakan ilmu yang mempelajari seni atau bagaimana menjamin suatu pesan sehingga pesan tersebut tidak dapat dimaknai oleh pihak lain yang tidak memiliki otoritas di dalamnya. Ada empat tujuan kriptografi antara lain kerahasiaan, integritas data, otentikasi dan non-repudiasi. Ada dua proses dalam kriptografi, enkripsi dan dekripsi, yang bertujuan untuk mengamankan pesan atau informasi. Proses pengamanan pesan atau informasi agar tidak dapat dipahami dan dibaca tanpa bantuan pengetahuan atau alat khusus disebut enkripsi. Sedangkan proses pengembalian informasi terenkripsi menjadi informasi yang dapat dipahami kembali disebut dekripsi (Primartha R, 2011). Ada dua jenis kriptografi, yaitu kriptografi klasik dan modern. Dalam penerapannya masyarakat lebih mengandalkan keunggulan kriptografi modern dalam proses pengamanan data, namun masih banyak masyarakat yang menggunakan kriptografi klasik dengan menggabungkan dua algoritma kriptografi klasik (Sadikin, 2012). Berdasarkan kunci yang digunakan, terdapat dua bagian dari kriptografi yaitu kriptografi simetris dan kriptografi asimetris. Perbedaan antara kedua kriptografi tersebut terletak pada kuncinya. Sistem algoritma simetris menggunakan kunci yang serupa, baik untuk proses enkripsi maupun dekripsi, seperti algoritma cipher klasik, stream cipher, DES, RC4 dan AES. Sedangkan algoritma asimetris menggunakan kunci yang berbeda dalam enkripsi dan dekripsi, seperti algoritma ECC, RSA, ElGamal, LUC, dan Rabin.

Algoritma DES mencakup sistem kriptografi simetris dan termasuk dalam jenis blok kode. DES beroperasi pada ukuran blok 64-bit. DES mengenkripsi pesan 64-bit asli menjadi pesan berkode

64-bit menggunakan 56 bit kunci internal. Ciphertext DES diperoleh dari berbagai proses substitusi dan transposisi plaintext sebanyak 16 kali (Kahate, 2013).

Pengertian Kriptografi

Kriptografi adalah ilmu yang mempelajari teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, otentikasi entitas, dan otentikasi asal data [2]. Kriptografi bertujuan agar informasi yang bersifat rahasia dan dikirim melalui suatu jaringan, seperti LAN atau internet, tidak dapat diketahui dan dimanfaatkan oleh orang lain atau pihak yang tidak berkepentingan. (Ashari Arief, 2016)

DES (Data Encryption Standart)

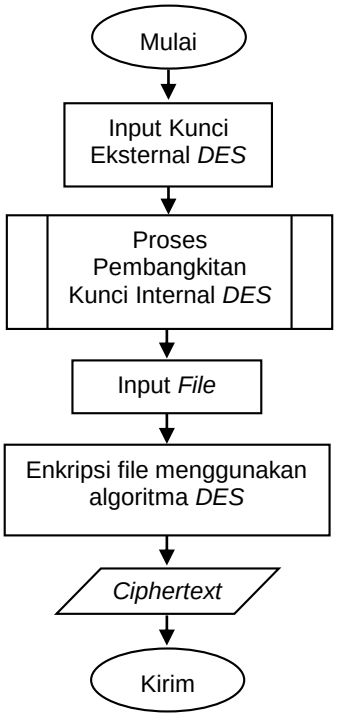
Penggunaan data sandi yang paling banyak didasarkan pada standard-standard data sandi (DES) yang diambil pada tahun 1977 oleh Standard-Standard Nasional Bureau, yang sekarang Institut Nasional Standard dan Tekhnologi (NIST), sebagai Standard Proses Informasi Umum. Untuk DES, data disandikan ke dalam 64 balok bit menggunakan 56 bit kunci. Transformasi algoritma 64 bitinput ke dalam satu serilangkah-langkah ke dalam 64 bitoutput. Langkah yang sama dengan kunci yang sama, digunakan untuk cadangan persandian. (Dadang Priyanto, 2016).

METODE PENELITIAN

Dalam penelitian ini peneliti menggunakan data teks input langsung dengan format *.txt, *.doc, dan *.Docx yang termasuk dalam tabel ASCII. Bahan penelitian diperoleh dari beberapa sumber, seperti jurnal, buku, prosiding, dan sumber bacaan elektronik.

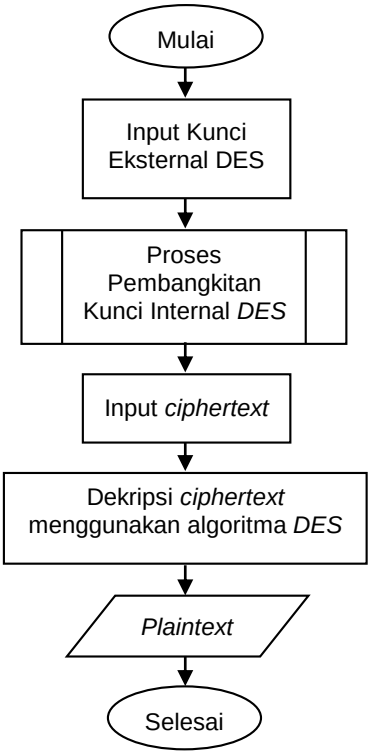
Rancangan Penelitian

Adapun *flowchart* dari penelitian ini dapat dilihat pada Ilustrasi di bawah ini.



Gambar 1. *Flowchart* Proses Enkripsi

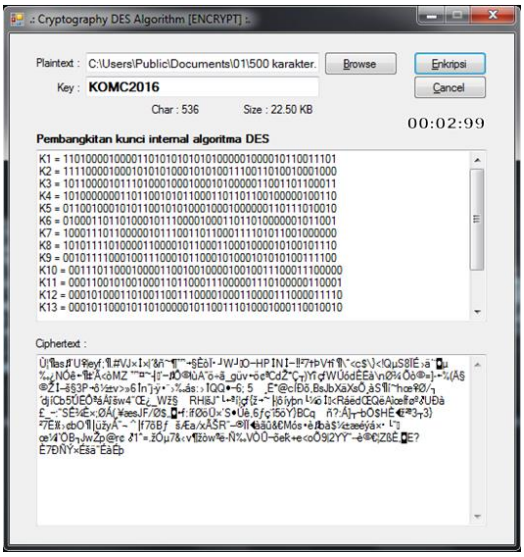
Jurnal Teknovasi
Volume 08, Nomor 01, 2021, 65 – 69
ISSN: 2540-8389



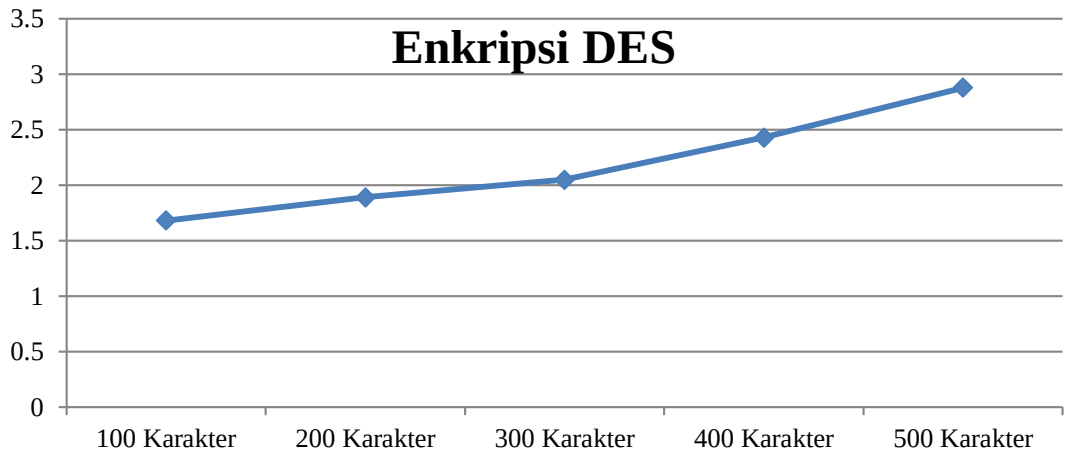
Gambar 2. *Flowchart* Proses Dekripsi

HASIL DAN PEMBAHASAN

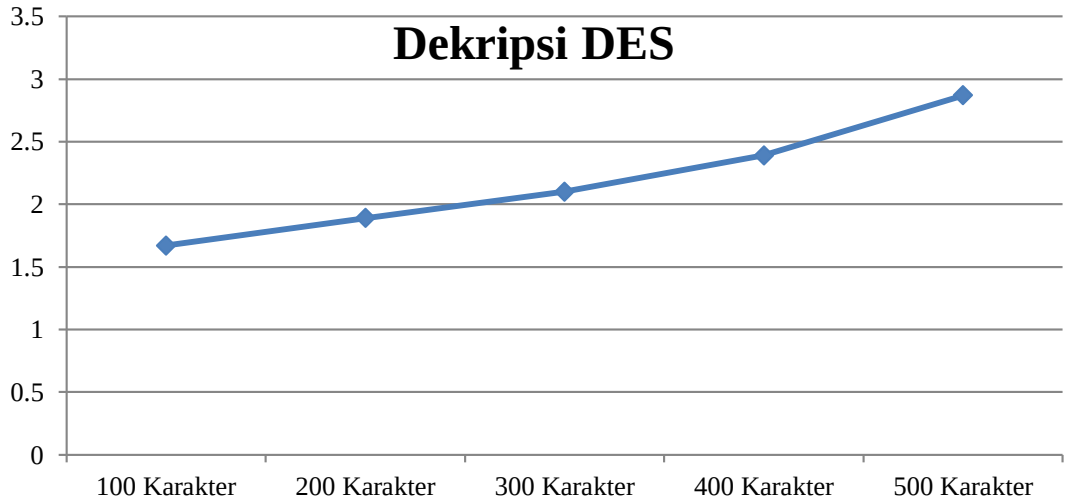
Pada tahap ini peneliti menguji waktu proses untuk mengetahui pengaruh ukuran karakter uji dan ekstensi file uji terhadap waktu proses enkripsi dan dekripsi menggunakan algoritma. Peneliti menguji file dengan ukuran 100, 200, 300, 400 dan 500 karakter. Pengujian dilakukan tiga kali untuk setiap file. Kemudian hasil dari proses tersebut akan dihitung. Berikut beberapa gambar hasil pengujian beberapa file berekstensi .doc:



Gambar 3. Contoh Salah Satu Hasil Uji Enkripsi File .doc Menggunakan Algoritma DES



Gambar 4. Grafik Panjang Karakter File .txt untuk Waktu Proses Enkripsi



Gambar 5. Grafik Panjang Karakter File .txt untuk Waktu Proses Dekripsi

Berikut penjelasan dari semua hasil tes diatas:
Hasil pengujian pada saat proses menunjukkan kesimpulan bahwa semakin banyak jumlah karakter file uji yang akan digunakan untuk proses enkripsi dan dekripsi maka semakin lama waktu yang dibutuhkan dalam proses algoritma. Hal tersebut dikarenakan proses enkripsi yang dilakukan oleh algoritma DES dilakukan per blok yang masing-masing blok terdiri dari 8 karakter atau 64 bit. Dan setiap 64 bit dilakukan proses yang sama. Kemudian menghasilkan proses komputasi yang semakin panjang karakternya maka semakin lama waktu prosesnya.

KESIMPULAN DAN SARAN

Kesimpulan

Dari hasil analisis algoritma DES pada keamanan file, peneliti dapat menyimpulkan bahwa:
Hasil pengujian pada proses *real time* menunjukkan kesimpulan bahwa semakin banyak jumlah karakter file uji yang akan digunakan untuk proses enkripsi dan dekripsi maka semakin lama waktu nyata yang dibutuhkan dalam proses algoritma.

Saran

Pada hasil penelitian ini, metode enkripsi yang diterapkan pada algoritma DES berhasil dilakukan karena dapat dibuktikan dengan plaintext yang diinput sebelum proses enkripsi sama dengan hasil proses dekripsi ciphertext. Namun dalam penentuan kunci internal DES hanya dibatasi sampai 8 karakter. Pengembangan dapat dilakukan dengan menggunakan kunci internal DES yang lebih dari 8 karakter sehingga dapat meningkatkan keamanan.

DAFTAR PUSTAKA

Ashari Arief & Ragli Saputra, 2016. Implementasi Kriptografi Kunci Publik dengan Algoritma RSA-CRT pada Aplikasi Instant Messaging, Scientific Journal of Informatics Vol. 3, No. 1, Mei 2016

Kahate, Atul. 2013. *Cryptography and Network Security*. Tata McGraw-Hill Education: New Delhi.

Novelan, M. S., Husein, A. M., Harahap, M., & Aisyah, S. (2018). SMS Security System on Mobile Devices Using Tiny Encryption Algorithm. Journal of Physics: Conference Series, 1007(1), 12037. Retrieved from http://stacks.iop.org/1742-6596/1007/i=1/a=012037

Primartha R. 2011. *Penerapan Enkripsi dan Dekripsi File Menggunakan Algoritma Data Encryption Standard (DES)*. Jurnal Sistem Informasi (JSI) 3(2):371-387.

Priyanto, D., & Azhar, R. (2016). SISTEM APLIKASI UNTUK KEAMANAN DATA DENGAN ALGORITMA 'DES' (Data Encryption Standard). MATRIK : Jurnal Manajemen, Teknik Informatika Dan Rekayasa Komputer, 16(1), 67-76.

Sadikin, R. 2012. *Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java*. Andi: Yogyakarta.